UtrechtLawReview

Remigijus Jokubauskas and Marek Świerczyński, 'Is revision of the council of Europe guidelines on electronic evidence already needed?' (2020) 16(1) Utrecht Law Review pp. 13–20. DOI: https://doi.org/10.36633/ulr.525

ARTICLE

Is revision of the council of Europe guidelines on electronic evidence already needed?

Remigijus Jokubauskas* and Marek Świerczyński†

On 30 January 2019 the Council of Europe adopted the first guidelines on electronic evidence in civil and administrative proceedings (hereinafter also 'Guidelines').[1] The authors question if the Guidelines already require some revisions. They also consider, whether the revised Guidelines should provide more practical advice to courts and legal practitioners related to electronic evidence. Several aspects have been identified regarding the use of the Guidelines by the courts in particular with the regard to the rapid development of online dispute resolutions systems and use of artificial intelligence algorithms in judicial systems. Both authors took an active part in the preparatory works of the Guidelines and believe it is in the interest of justice that the Guidelines should be regularly updated addressing and reflecting technological developments, new business models and evolving case-law.

Keywords: electronic evidence; guidelines; online dispute resolutions systems; digital divide; artificial intelligence; cloud computing; blockchain

1. Introduction

The Council of Europe adopted the Guidelines on electronic evidence in civil and administrative law only recently, on 30 January 2019. An indispensable document to the Guidelines is the Explanatory Memorandum (hereinafter 'Explanatory memorandum') which clarifies the provisions of the Guidelines and reveals the sources which were used in the Guidelines. The aim of this paper is to determine whether the revision of the Guidelines is already needed. This is of particular importance as the Guidelines need to be updated from time to time and the first experience of their application should be used for this purpose. Noteworthy; the Council of Europe is working on the guidelines of Online Dispute Resolution (ODR) that also affects electronic evidence.[2] Moreover, the increasing need to address electronic evidence in civil and administrative proceedings show the development of the regulation of the European Union law. The Regulation on electronic identification and trust services for electronic transactions in the internal market (hereinafter 'eIDAS regulation') establishes various means of electronic evidence (such as trust services, electronic seals, electronic time stamp, electronic registered delivery service, electronic signature).[3] Moreover, the eIDAS regulation recognizes the fundamental principle that electronic evidence should not be denied legal effect

* Remigijus Jokubauskas, PhD in Law candidate at Mykolas Romeris university (Lithuania), email: remigijus@jokubauskas.org.

† Dr. hab. Marek Świerczyński, Professor of Civil and Private International Law, University of Cardinal Stefan Wyszynski in Warsaw (Poland), Insitute of Legal Studies, expert consultant to the Council of Europe, email: m.swierczynski@uksw.edu.pl.

[1] Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (Adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers' Deputies), 30 January 2019, CM(2018)169-add1final.

[2] Already in 2016 a study was undertaken on the feasibility for the European Committee on Legal Co-operation (CDCJ) of the Council of Europe to undertake an activity on online dispute resolution (ODR) mechanisms with reference to Articles 6 and 13 of the European Convention on Human Rights (ECHR). As a follow-up to this feasibility study, the CDCJ decided to start, in 2017, work on the preparation of a technical study as a first step of the activity. This technical study has been completed and presented to CDCJ at its 93rd plenary meeting (14–16 November 2018) which approved its publication on its website. The activity is continued with the preparation, by the end of 2020, of draft guidelines aiming at ensuring the compatibility of ODR mechanisms with Articles 6 and 13 of the ECHR. See https://www.coe.int/en/web/cdcj/online-dispute-resolution-mechanisms [Accessed: 2 January 2020].

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC OJ L 257, 2014.

and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form.[4] Also, the Proposal for the amendment of the Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters by the European Commission establishes that modern communications technology,[5] in particular videoconferencing which is an important means to simplify and accelerate the taking of evidence, is currently not used to its full potential. Therefore, the proposal recognizes that the direct taking of evidence by videoconference should be one the means of taking of evidence. The equal treatment and evidentiary value of electronic evidence should be ensured.[6]

The authors do not intend to just present or summarize the existing Guidelines or their adopting procedure. The readers of this paper are encouraged to read both the guidelines and the explanatory memorandum.[7] The focus of this paper is on the possible revisions that may be required. The references to the original version of the Guidelines is made only if required. Since both authors were the members of the drafting group preparing the Guidelines, we also would like to comment on the sections removed during the final stage of preparation. We are of opinion that some points and definitions should be reinstated to the Guidelines, as their removal was not sufficiently justified. This mainly relates to the fundamental principle of human rights. Additionally, the Guidelines should directly refer to the use of blockchain and cloud computing in securing or handling electronic evidence.

Beside the general question of the possible revision, a number of additional specific academic questions that need to be answered. Should the revised Guidelines provide more practical advice to courts and legal practitioners related to electronic evidence? Should such guidelines be aimed at harmonisation of the national legislation of Member States or continue to be established at the level of general principles accommodating all the different legal systems? Should the new EU regulations on electronic evidence and ongoing work at the Hague Conference be used as a source of inspiration for developing revised guidelines?

2. The main reasons for revising the guidelines (new challenges)

The courts and administrative authorities daily handle cases concerning electronic evidence that have been submitted by the parties and other persons involved in civil or administrative proceedings.[8] In recent years, this process has accelerated. This is also directly related to the development of Online Dispute Resolutions (ODR) systems, more often in parallel with introduction of artificial intelligence algorithms (i.e. data analysis) to the judicial systems. ODR are to be defined as mechanisms used for dispute resolution that is carried out at a distance through the use of computers and the internet.[9] Both of these factors strongly enhance digitalisation of the procedures and their importance.[10] It may also revolutionize access to justice for litigants, for example to persons who now find it hard to access courts.[11] Digitalisation also improves the justice

[4] Article 25(1), 35(1), 41(1), 43(1) of the eIDAS regulation.

[5] Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (COM/2018/378 final).

[6] Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (SWD/2018/285 final).

[7] The main part of the document consists of 35 detailed guidelines contained in separate sections. It's available on the Council of Europe webpage: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c [Accessed: 2 January 2020] and the Explanatory Memorandum to the Guidelines is available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0e [Accessed: 2 January 2020]. The Explanatory memorandum explains the Guidelines in detail and provides examples of the relevant case law, national laws and legal teachings.

[8] M. Biasiotti, J. Bonnici, J. Cannataci, F. Turchi, *Introduction: Opportunities and Challenges for Electronic Evidence*, in: *Handling and Exchanging Electronic Evidence Across Europe*, ed. M. Biasiotti, J. Bonnici, J. Cannataci, F. Turchi, Cham 2018, p. 4. For further information on the digital transformation of the civil justice see A. Uzelac, C. H. van Rhee (eds.), *Transformation of Civil Justice, Ius Gentium: Comparative Perspectives on Law and Justice*, Springer International Publishing 2018.

[9] For example in Poland the procedure for payment orders is fully electronic. The claim is submitted through an individual account opened in a dedicated IT platform. All acts and documents are available online. In Lithuania videoconferencing can be used in civil procedures as each court is equipped with at least one video conference room and every court room is equipped with an audio equipment.

[10] *Online Dispute Resolution and Compliance with the Right to a Fair Trial and the Right to an Effective Remedy (Article 6 and 13 of the European Convention of Human Rights). Technical Study on Online Dispute Resolution Mechanisms* – prepared by Prof Julia Hörnle, CCLS, Queen Mary University of London, Matthew Hewitson (South Africa) and Illia Chernohorenko (Ukraine), Strasbourg, 1 August 2018, CDCJ(2018)5.

[11] On this topic see excellent monograph of J. Hörnle, *Cross-border Internet Dispute Resolution*, Cambridge University Press 2009.

system by providing cheaper means to resolving disputes.[12] This process affects also national procedures on electronic evidence.

The new challenge that is not addressed in the Guidelines is rapid emergence of artificial intelligence (AI). AI is a broad area of ICT technology that enables automated reasoning.[13] It allows to make automated decisions, recommendations and forecasts effective, accessible and affordable.[14] In practice, this means that many civil and administrative proceedings based on time-consuming judicial work can be automated.[15] It may be based on repeating patterns of factual scenarios and the legal categorization of disputes.[16] Currently, AI components are being introduced in judicial systems particularly regarding the data analysis.[17] This also means that the rules on electronic evidence should be streamlined in order to allow for implementation of the AI in the proceedings. For example, AI is not able to process data presented by the parties in written form (printouts – in this respect see guideline no 9 in the original Guidelines).

Electronic evidence differ in many respects from other types of evidence.[18] Electronic evidence (also called digital evidence) can be text, videos, photos or sound recordings.[19] Data can come from a variety of sources such as mobile phones, websites, computers or GPS recorders.[20] This also includes data stored at a distance within the cloud computing or increasing use of AI systems. A typical example of electronic evidence is electronic data derived from an electronic device that contains relevant metadata.[21] Related to this issue are the technologies being nowadays more often used to secure evidence, such as distributed registers (*blockchain*).[22,23] Blockchain is a relatively new technology that can provide greater confidence and security of electronic evidence.[24] It can be defined as a distributed register, which contains a list of records (blocks), connected and secured by cryptography and registered in a decentralised equivalent network. This makes blockchain technology very useful for evidential purposes. However, there is no direct reference to blockchain in the Guidelines. Only the Explanatory memorandum mentions this technology as inherently

[12] J. Hörnle, *Encouraging Online Alternative Dispute Resolution (ADR) in the EU and Beyond*, European Law Review 2013, Volume 38 (2), pp. 187–208.

[13] Recommendation of the OECD Council on Artificial Intelligence, OECD/LEGAL/0449, Adopted on: 22/05/2019, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [Accessed: 2 January 2020].

[14] Already number of expert studies on AI use in judicial systems were published. In this respect we recommend CoE recent document: *A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework. Prepared by the Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence* (MSI-AUT). Rapporteur: Karen Yeung, DGI(2019)05.

[15] M. Scherer, *Artificial Intelligence and Legal Decision-Making: The Wide Open?*, Journal of International Arbitration 2019, vol. 36, no. 5, pp. 539–574.

[16] D. Carneiro et al., *ODR: an Artificial Intelligence Perspective*, Artificial Intelligence Review 2014, Volume 41, pp. 211–240.

[17] This is being further elaborated by the European Commission's high-level expert group on artificial intelligence. In particular see the document "*A Definition of AI: Main Capabilities and Scientific Disciplines. Definition developed for the purpose of the deliverables of the High-Level Expert Group on AI Brussels*, 18 December 2018; available at https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai [Accessed: 2 January 2020].

[18] We recommend the following monographs on the issue of electronic evidence, as we use them in the preparation of the original Guidelines: George L. Paul, *Foundations of Digital Evidence* (American Bar Association, 2008), Paul R. Rice, *Electronic Evidence – Law and Practice* (2nd edn, American Bar Association, 2009), Allison Stanfield, Computer Forensics, *Electronic Discovery & Electronic Evidence* (LexisNexis Butterworths, 2009), Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2017), Stephen Mason, ed, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008).

[19] J. Bonnici, M. Tudorica, J. Cannataci, *The European Legal Framework on Electronic Evidence: Complex and in Need of Reform*, in: *Handling and Exchanging Electronic Evidence Across Europe*, ed. M. Biasiotti, J. Bonnici, J. Cannataci, F. Turchi, Cham 2018, p. 190.

[20] G. Weir, S. Mason, *The sources of electronic evidence*, in: *Electronic Evidence*, (ed. S. Mason, D. Seng), London 2017, pp. 14–17.

[21] G. Weir, S. Mason, *The sources...*, p. 10.

[22] On the current uses of blockchain technologies in the legal systems see further: *Distributed Ledger Technology: beyond block chain, A report by the UK Government Chief Scientifc Adviser, Government Office for Science*, London 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/ file/492972/gs-16-1-distributed-ledger-technology.pdf [Accessed: 2 January 2020].

[23] M. Pilkington, *Blockchain Technology: Principles and Applications, Research Handbook on Digital Transformations*, Edward Elgar 2016, https://ssrn.com/abstract=2662660 [Accessed: 2 January 2020].

[24] R. Neisse, G. Steri, I. Fovino, *A blockchain-based approach for data accountability and provenance cracking*, w: *Proceedings of the 12th International Conference on Availability, Reliability and Security*, Reggio Calabria, Italy, 29 August–01 September 2017, pp. 14:1–14:10, available at https://doi.org/10.1145/3098954.3098958 [Accessed: 2 January 2020] and M. Vukolic, *Rethinking permissioned blockchains*, w: *ACM Workshop on Blockchain, Cryptocurrencies and Contracts* (BCC 2017), April 2017, available at http://vukolic.com/rethinking-permissioned-blockchains-BCC2017.pdf [Accessed: 2 January 2020]. See also K. Knnapas, *From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of de lege ferenda?*, in: *The Future of Law and eTechnologies*, (ed. T. Kerikmae, A. Rull), Cham 2016, p. 111.

resistant to data modification. This is one of the main new issues that should be further addressed in the revised Guidelines.

Except the Guidelines only a few legal documents which have been adopted to facilitate the handling of electronic evidence in civil and administrative proceedings at international, European and national level so far.[25] A gap still exists in both law and judicial practice regarding the key technological principles of dealing with electronic evidence, in particular, when we speak about the use of cloud computing, blockchain or AI algorithms in securing, submitting and analysing the electronic evidence.[26] That is why the need for revision of the Guidelines is particular importance. They should be adapted to the current stage of development of court digitalisation. Because of such reasons, we are in opinion that the first revision should be accompanied with adopting both the guidelines and the definitions to such new technologies like cloud computing, blockchain or AI algorithms.

The authors believe that evidence by algorithm, cloud computing, blockchain or otherwise electronically might be reliable and trustworthy enough in civil and administrative proceedings. What matters most in practice is how these types of evidence may be collected and what admissibility requirements shall be established. They may be collected by using special software programs which in means that some expertise may be required. However, each of these specific evidences has its own peculiarity. For instance, blockchain is inherently resistant to modification of the data. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority. This makes blockchain suitable for the evidencing purposes. One of the possibilities to ensure lawfulness of a digital record electronically registered in a blockchain could be a declaration of a qualified person. Similarly, authentication of evidence by cloud computing and algorithm may be useful and a first step in the authentication process. However, if the authentication is not sufficient, expertise may be particularly relevant.

3. Possible new sections to be added to the guidelines

We are of opinion that a number of new problems should be addressed by revised Guidelines. First of all, the key principle on the human rights should be reinstated to the fundamental principles of the Guidelines. It's removal at the final stage of the drafting of the Guidelines sounds strange since the Guidelines were prepared by the Council of Europe in accordance with the case law of the European Court of Human Rights (hereinafter ECtHR).

One may argue that it may be self-evident that the Guidelines should be read together with other guidelines and the ECHR case law. Nevertheless, the Guidelines regulate a particularly distinct type of evidence to which the application of the general rules of human rights protection and the case law of the ECHR may require some particular view. Moreover, the explicit reference to the human rights (such as the right to a private life) may draw practitioners' attention and require to consider the protection of human rights when dealing with electronic evidence in each case.

[25] There are only some general and already outdated regulations, such as: The Model Law on Electronic Commerce adopted by the Commission on 12 June 1996, following its 605th meeting and adopted by the General Assembly in Resolution 51/162 at its 85th plenary meeting 16 December 1996, including an additional article 5 bis as adopted by the Commission at its 31st meeting in June 1998. The Model Law on Electronic Signatures was adopted by the Commission at its 727th meeting on 5 July 2001. See also guidelines adopted outside Europe, i.e. Commonwealth Draft Model Law on Electronic Evidence and Electronic Evidence: Model Policy Guidelines & Legislative Texts (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean, International Telecommunication Union Telecommunication Development Bureau, Geneva, 2013). Number of such guidelines exist in case of electronic evidence in criminal cases, comp. M. Biasiotti, J. Bonnici, J. Cannataci, F. Turchi, *Introduction...*, p. 8 and f. See also Recommendation No R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies; European Certificate on Cybercrime and Electronic Evidence (ECCE project, Cybex and European Commission, 2007), The Admissibility of Electronic Evidence in Court (EU AGIS 2005 Programme and Cybex, 2006); UNODC Comprehensive Study on Cybercrime (United Nations, New York, Draft – February 2013) or Bert-Jaap Koops and Morag Goodwin report: *Cyberspace, the cloud and cross-border criminal investigation The limits and possibilities of international law*, Commissioned by WODC, Ministry of Security & Justice (Tilburg University, December 2014). See M. Biasotti, *A proposed electronic evidence exchange across the European Union*, Digital Evidence and Electronic Signature Law Review, 14 (2017), pp. 1–12; B. Hancock, *US and Europe Cyber crime Agreement Problems*, Computers and Security 19/4 (2000), pp. 306–307; C. Coleman, *Security Cyberspace—New Laws and Developing Strategies*, Computer Law and Security Report 19/2 (2003), pp. 131–136; I. Walden, *Harmonising Computer Crime Laws in Europe*, European Journal of Crime, Criminal Law and Criminal Justice 12/4 (2004), pp. 321–336; M. Nuth, *Taking Advantage of New Technologies: For and Against Crime Computer Law and Security Report*, Computer Law & Security Review 24 (2008), pp. 437–446; N. Katyal, *Criminal Law in Cyberspace*, University of Pennsylvania Law Review 149/4 (2001), pp. 1003–1114; S. Wang, *Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crimes*, Computer Standards and Interfaces 29 (2007), pp. 216–223.

[26] Such aspects are missing in the original CoE study on electronic evidence: "*The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof. A comparative study and analysis*" – report prepared by Stephen Mason assisted by Uwe Rasmussen. Strasbourg, 27 July 2016, CDCJ(2015)14 final.

We believe that the Guidelines must be drafted in the way to strengthen the efficiency and quality of justice. It is particularly important, as the rules on electronic evidence adopted so far in the member states are not sufficiently focused on procedural safeguards but rather on having a dispute resolved in an effective manner in a cost-efficient way.[27] This is a challenge to ensure that rules on electronic evidence are compliant with the right to a fair trial which is established in Article 6 of the European Convention on Human Rights. It is crucial that the Guidelines contribute to more efficient access to justice. The revised version of the Guidelines should be drafted in such a way that the issue of the digital divide is adequately addressed. It is important to establish that parties to the proceedings are not placed in a disadvantageous position because of their lack understanding of how the technologies are used. Procedural rules on electronic evidence should be as user-friendly as possible in a meaning that it does not operate in a manner that would be likely to prejudice the interests of any of the parties.

As mentioned above, the fundamental principle of the Guidelines that was deleted in the final stage of preparation referred to the rule of law and inadmissibility of electronic evidence that has been obtained in an unlawful manner (e.g. as a result of a breach of privacy or data confidentiality rules). An example is the seizure of an electronic device without a court order required by law, as well as evidence obtained by a party through hacking into an IT system. For example, it follows from the case-law of the ECtHR that evidence gathered as a result of an infringement by an employer of the principles of protecting the privacy of the employee may be inadmissible due to a breach of the principle of proportionality. In the fundamental case *Bărbulescu v. Romania* the Grand Chamber of the ECtHR found that the Romanian courts, in reviewing the decision of the employer to dismiss the employee after having monitored his electronic communications, failed to strike a fair balance between the employee's right to respect for his private life and correspondence and his employer's right to take measures in order to ensure the smooth running of the company.[28] The evidence gathered in such way (by violation of the right to private life) is not compatible with the right to a fair trial and should not be admissible. Nevertheless, a difficult question arises when electronic evidence is gathered without a person's knowledge and acceptance, but it shows that the person has committed a crime. In the recent case *López Ribalda and others v. Spain* the Grand Chamber of the ECtHR found that surveillance of employees by hidden cameras (about which the employees did not know) was in accordance with the right to private life since the video footage was used only to trace those responsible for the r losses of goods from the shop and to take disciplinary measures against them.[29] Also, the court found that the national rules provided significant procedural safeguards in this case. Therefore, the revised version of the Guidelines should include this significant development in the collection of electronic evidence.

Another sections that requires to be more elaborated in the Guidelines is how the authenticity or integrity of electronic evidence can be challenged (compare existing guidelines no. 18–24 of the original Guidelines), in particular with regard to evidence derived from cloud computing, blockchain or using AI algorithms. The Guidelines may provide appropriate specific mechanisms, e.g. in the form of the addendum to the Guidelines explaining blockchain characteristics, in order to facilitate such a challenge. Moreover, the Guidelines should be clear on that parties should be fully permitted to challenge expert evidence where such evidence is likely to determine the outcome of the proceedings (compare exiting guideline no 18 of the original Guidelines). In this regard the principles of legal certainty and protection of legitimate expectations of the parties point towards parties being able to rely on previous decisions made by a court where the facts of the case concerned were similar to those in the current proceedings. It is recommended that parties are able to structure their evidence based on such decisions. Therefore, for the reasons of legal certainty and consistency, the revised version of Guidelines should have regard to such precedence decisions, departing from them only where there are good and sufficient reasons for doing so. Noteworthy, the ECtHR has accepted that the principle of legal certainty implies that a party relying on the assessment made by a court in a previous case on an issue also arising in the case at hand may legitimately expect the court to follow its previous ruling, unless there is a valid reason for departing from it (Siegle v. Romania, §§ 38–39, and Rozalia Avram v. Romania, §§ 42–43).[30]

[27] D. Vitkauskas, G. Dikov, *Protecting the right to a fair trial under the European Convention on Human Rights: A handbook for legal practitioners*, Council of Europe 2017, available from: https://rm.coe.int/protecting-the-right-to-a-fair-trial-under-the-european-convention-on-/168075a4dd [Accessed: 2 January 2020].

[28] ECtHR judgment of 5 September of 2017 in case *Bărbulescu v. Romania*, petition No. 61496/08.

[29] ECtHR judgment of 17 October 2019 in case *López Ribalda and others v. Spain*, petitions No. 1874/13 8567/13.

[30] Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (civil limb), updated to 31 December 2018, Council of Europe/European Court of Human Rights, 2018.

The new ways to identify the source of evidence, i.e. in case of evidence derived from blockchain, use of AI algorithms or cloud computing, should be presented in the Guidelines as well. The missing points in the existing version of the Guidelines are exactly the identification of the source of the evidence in case of blockchain, cloud computing or AI algorithms. It is important that there is no issue of fraudulent identities. Separation of the digital identity from the physical generate problems related to the source of evidence. In this regard the Guidelines could provide explicit guideline that confirmation of identity by the payment system operator may be used as an identification mechanism.

Even more focus in the revised version of the Guidelines should be made on the awareness of the potential probative value of metadata.[31] Metadata is currently defined in the Guidelines as data relating to other data. A picturesque metaphor is to call it as the 'digital fingerprint' of electronic evidence. It may contain important evidential data, such as the date and time of creation or modification of a file or document, data on the author or the date and time of sending. Due to the technological difficulties the revised version of the Guidelines should provide examples how metadata should be collected and assessed in practice. Since collection of metadata may require certain additional computer programs and specific knowledge, the Guidelines could specify how the participants in the proceedings should handle this practical task. Also, since metadata may be manipulated, the Guideline could explain how the courts should assess metadata and find whether it had been changed.

The Guidelines should also cover the problem of manipulation with electronic evidence and the ways to identify whether evidence has been tampered (compare existing guidelines no. 10–11 of the original Guidelines). In our opinion the burden of establishing the reliability of electronic evidence carried by the party seeking to rely on it (for example, by providing expert affidavit) should be regulated in the revised Guidelines. Judges and legal practitioners must also be mandatory trained (and not just informed) on the evolution of information technology and processes which may impact on the value of electronic evidence.

One of the most difficult part that needs to regulated is the determination of the law applicable to evidence obtained in relation to cross-border cases and the remedies available, for example in the case of failure to respect court authority and integrity of court proceedings (contempt of court) or perjury. Existing guidelines no. 12–13 are not satisfactory in this regard, although we understand that this issue is highly complicated and require extensive additional work. However, we believe that this is exactly the right challenge for the revised guidelines to provide standards for transmission of electronic evidence both between foreign courts.[32] It is helpful that the European Union is working parallel on such new standards. Nevertheless, the task of Council of Europe is not to repeat or extend European Union solutions to other states but rather to elaborate more universal rules. One should take into consideration that although the use of the evidence may be purely national, it is increasingly likely to be cross-border. An example is the location in a foreign country of the cloud computing or blockchain infrastructure used to process or store data, or the location of the provider that allows storage or processing of data. The revised version of the Guidelines should make stronger emphasis on direct cooperation between courts and cloud service providers in cross-border cases and give specific guidelines what should be results of such cooperation (e.g. on securing on seizing the electronic evidence).[33]

Cloud computing is an exact example of cross-border technology by nature.[34] Sharing data within the cloud means storing different parts of the database on different servers, which may be located in different physical locations.[35] Storing data that may constitute electronic evidence in the cloud has already become a common practice. The global nature of the Internet and the growing use of cloud services make it increasingly difficult to assume that access or processing data is purely national. The problem is that there are significant differences between national procedural rules on the taking of evidence abroad. The courts using evidence abroad have to take these differences into account.

[31] B. Schafer, S. Mason, The Characteristics of Electronic Evidence, in: Electronic Evidence: Disclosure, Discovery and Admissibility, ed. S. Mason, P. Argy, & D. Begg, Butterworth 2010, p. 28.

[32] D. Svantesson, *Law enforcement cross-border access to data*, Preliminary Report, November 2016.

[33] D. Jerker, D. Svantesson, L. van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law Security Review 2016, vol. 32, pp. 671–682.

[34] B. Sujecki, *Private International Law Aspects of Cloud Computing – A European Perspective*, w: *X-lecie. Księga pamiątkowa z okazji dziesięciolecia Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, Wrocław 2012, pp. 236–248.

[35] M. Vincent, N. Hart, *Legal issues in the cloud,* Computers & Law 2011, vol. 79, pp. 3–4.

The foregoing is not intended to represent the exhaustive list of issues that arise in the context of electronic evidence and which could form the subject matter of revised guidelines. It should address and reflect all relevant and recent technological developments, new business models and evolving case-law.

We consider that revised version of the Guidelines should not establish binding legal standards. By its very nature, it is non-binding instrument (*soft law*).[36] It does not aim to harmonise member states' national legislation. Nor should the guidelines be interpreted as prescribing a certain legal value to electronic evidence. The Guidelines should be formulated in such a general way as to take into account the different legal systems of the member states of the Council of Europe.

Nevertheless, it is possible and recommended that they have the character of a practical toolbox. The guidelines should not be only a declaration of principles but provide practical guidance. For this reason, we are of opinion that the Guidelines could be supplemented with more technical and elaborated addendums. An example could be the list of challenges relating the use of cloud computing in securing and seizing electronic evidence.[37]

4. Conclusions

The Guidelines adopted by the Council of Europe is the first international document which explains how courts should handle electronic evidence in civil and administrative proceedings. It was adopted in accordance with the national laws of the Member States of the Council of Europe and the human rights standards established in the case law of the ECtHR. Nevertheless, the authors believe that due to the rapid changes in the technology and legal regulation of electronic evidence the Guidelines should be revised. Also, the current version of the Guidelines does not address some particularly importance aspects of electronic evidence.

Electronic evidence related to cloud computing, blockchain, AI algorithms is scarcely explained in the Guidelines or the Explanatory memorandum. However, these types of electronic evidence are particularly challenging to the courts and legal practitioners. All of these types of electronic evidence refer to the court digitalisation and there is a lack of international standards which regulate these questions. The revised version of the Guidelines should not only define these types of electronic evidence, but also explain the peculiarities how they should be collected and assessed in practice.

The authors also suggest that new sections could be added to the Guidelines. The current version of the Guidelines and the national regulation of the member states are not sufficiently focused on procedural safeguards but rather on having a dispute resolved in an effective manner in a cost-efficient way. Nevertheless, the development of the case law of the ECtHR regarding the collection of electronic evidence (by video surveillance) and protection of the right to a private life is particularly important. The collection of electronic evidence is tightly linked with the right to a private life. The Guidelines should address the need to protect the right to a private life with the right to collect electronic evidence and how the fair balance between these two rights shall be established.

Another crucial area which should be addressed in the revised version of the Guidelines is cross-border of transmission of electronic evidence. Often electronic evidence may be located in another country than the court which handles the case. In such case there is a need to transmit information or collect it in cooperation with a foreign court (other institutions and even private entities). The existing version of the Guidelines is not satisfactory in this regard, though we understand that this issue is highly complicated and require extensive consideration. However, this is exactly the right challenge for the revised version of the Guidelines to provide standards for transmission of electronic evidence both between foreign courts.

Competing Interests

The authors have no competing interests to declare.

[36] We do not believe that adoption of convention is possible. On this matter see S. Mason, *A proposed Convention on Electronic Evidence*, Pandora's Box, 2016, pp. 153–155 (http://www.jatl.org/pandoras-box/) S. Mason, *Towards a global law of digital evidence? An exploratory essay*, Revista de Concorrência e Regulação, Ano VI, number 23–24, julho– dezembro 2015, s. 239–258, S. Mason, *Amicus Curiae The Journal of the Society for Advanced Legal Studies*, Issue 103, Autumn 2015, pp. 19–28.

[37] Comp. "*Unleashing the Potential of Cloud Computing in Europe*" Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 27.9.2012 COM(2012) 529 final, SWD(2012) 271 final.

How to cite this article: Remigijus Jokubauskas and Marek Świerczyński, 'Is revision of the council of Europe guidelines on electronic evidence already needed?' (2020) 16(1) Utrecht Law Review pp. 13–20. DOI: https://doi.org/10.36633/ulr.525

Published: 26 May 2020

Utrecht Law Review is a peer-reviewed open access journal published by Utrecht University School of Law.

OPEN ACCESS